Crédit photo : CHU Grenoble Alpes - Agence TOPO

ADVENS
DES SOLUTIONS MANAGÉES, PAS À PAS

Il y a 3 ans, Advens se positionnait sur une offre packagée de SOC (Security Operations Center) managé pour les établissements de santé. Face au succès de la formule et à l'accroissement des menaces, la société a renouvelé cet été son marché avec la centrale UniHA (CAIH). Le périmètre de protection est encore étendu, pour plus de sécurité.

FOURNIR UN SERVICE 24H/24, 7J/7

En 2019, l'initiative part d'un constat simple. La plupart des postes de travail des établissements de santé sont alors équipés du système d'exploitation Windows 7 dont le support arrive à expiration. « 70% des 150 000 endpoints que nous équipions étaient concernés, souligne Thomas Jan, directeur général adjoint en charge de la stratégie numérique chez UniHA (CAIH).

Nous avons alors réfléchi pour aider ces établissements à opérer une mitigation du risque. » Pour les protéger, il n'y avait pas de migration simple, du fait d'un parc applicatif très hétérogène.

Il a donc fallu trouver une solution adéquate. Cela s'est traduit par une offre d'EDR (Endpoint Detection and Response) managé, capable de garantir le maintien en conditions de sécurité et de fournir de l'alerte si besoin. Les adhérents de la CAIH et du club RSSI Santé ont été sondés pour déterminer quels établissements seraient potentiellement intéressés pour cumuler en volume et ainsi obtenir les meilleurs prix. « Nous avons énormément travaillé avec le terrain, souligne Thomas Jan. Nous avons ainsi créé une offre disruptive, élaborée pour et avec les professionnels. »

D'où le choix d'une solution de services opérés à 360° permettant d'alerter, de diagnostiquer, d'établir des plans d'actions et de réaliser les premiers secours.

« Les établissements de santé n'ont pas les ressources nécessaires en interne pour assurer leur sécurité, ni en termes de disponibilité (24h/24 et 7j/7), ni en termes de compétences, constate Jacky Grisey, SOC manager en charge du run service (service de routine) chez Advens. L'idée était donc de démocratiser l'EDR managé en obtenant une solution adaptable à la maturité et aux besoins de chacun et à des prix bas car nous jouons sur de gros volumes. »

A la clé, l'offre proposée est en effet très modulable. Articulée autour de nombreuses unités d'oeuvre, elle s'applique par le biais de bons de commande, très faciles à mettre en place pour les hôpitaux. « Nous ne vendons pas une solution, nous vendons un service », souligne Thomas Jan.

La formule a rapidement rencontré son public. A l'heure actuelle, 40% des GHT ont recours à ce marché. Les souscriptions se sont accélérées en 2022 et 2023, sous l'effet des attaques et d'un accompagnement renforcé de l'Etat, notamment avec le plan France Relance. « Nous sommes passés de 90 à 150 clients en deux ans », se félicite Jacky Grisey. Forts de ce succès, les acteurs du marché ont opté pour un renouvellement en juillet dernier.

VERS TOUJOURS PLUS PROTECTION

La nouveauté de ce second marché réside dans l'extension de son périmètre, nous y reviendrons. Mais les fondements sont restés les mêmes, à savoir : le caractère agnostique de la solution et sa souveraineté.

Le GHT de la Réunion a opté pour une solution de SOC managé avec un EDR managé en 2020. Pour son RSSI, Stéphane Duchesne, l'aspect agnostique de la formule est incontournable. « J'ai tout intérêt à ce que la solution ne soit pas dépendante du SOC, et inversement. Sur cette question, Advens est très ouvert. S'il arrive qu'ils ne couvrent pas certaines solutions, il ne sont pas fermés. Je leur soumets le cas et ils réagissent très rapidement ». Un véritable confort pour les établissements qui ont donc le choix de la solution et ne sont pas dépendants d'un éditeur. « Nous devons être en mesure de proposer la solution la plus adaptée au client, selon sa maturité et les fonctionnalités qu'il recherche », complète Frédéric Descamps, Market Manager Public & Healthcare.

La question de la souveraineté quant à elle a toujours été une attente du secteur de la santé, qui s'est renforcée ces dernières années. RGPD, directives européennes NIS, labellisation, de nombreux critères poussent vers des solutions souveraines. La formule « SOC mutualisé santé par CAIH opéré par Advens » répond en tout point à ces attentes et notamment aux critères du plan national CARE (Cybersécurité Accélération et Résilience des Etablissements, porté par l'Agence du Numérique en Santé).

Mais c'est désormais sur son périmètre qu'elle va plus loin. Avec ce second marché, de nouvelles unités d'œuvre font leur entrée. NDR (Network Detection and Response), protection des mobiles, management de la vulnérabilité, protection des messageries, le champ couvert est encore plus large. Un CSIRT (Cyber Incident Response Team) est également mis en place pour prendre en charge les crises. Il peut déployer des moyens sur site si besoin. « Ce second marché étend considérablement la palette de l'offre, indique Ivan Paturel, directeur technique et RSSI du CHU Grenoble-Alpes et du GHT Alpes Dauphiné. Sondes réseau, équipements périmétriques, il intègre une supervision plus exhaustive sur la détection. C'est ainsi qu'on peut limiter in fine l'impact des attaques. »

UN DÉPLOIEMENT EN DEUX TEMPS

A Grenoble comme à la Réunion, c'est donc la fin du support de Windows 7 qui a provoqué le changement. « Nous sommes alors passé de l'utilisation d'une solution de sécurité à un service de surveillance, résume Stéphane Duchesne. Il y a eu toute une gestion du changement à réaliser. A ce titre, tout était prévu par Advens. » Plaquettes, accompagnement, packages pour désinstaller et installer en toute autonomie, poste par poste.

Le déploiement quant à lui s'est fait en deux phases. Durant près de 6 mois, Grenoble a ainsi tout d'abord déployé la solution sur l'ensemble de ses 8 500 postes et 1 400 serveurs en mode "détection". Ce mode cherche à faire des ajustements sur les faux positifs. L'EDR fait des signalements lorsque sont relevés des comportements anormaux mais aucune mesure de protection n'est réalisée. Il peut en effet s'agir de comportements normaux, liés à l'activité de certaines applications. Les équipes d'Advens, en collaboration avec les équipes du CHU, ajustent et qualifient au fur et à mesure les alertes pour optimiser le paramétrage de l'EDR. Ensuite, les faux positifs diminuent et le mode "protection" peut être appliqué. L'intégralité du parc est alors protégée et il est procédé à une mise en quarantaine si une anomalie est détectée sur un poste. « Le point fort à ce niveau est qu'en mutualisant les expériences de tous ses clients, le SOC a une connaissance fine des évolutions des applications de santé (pour déceler les faux positifs) et des attaques (pour bloquer au plus tôt) », souligne Ivan Paturel. La preuve (même si en la matière, il ne faut jamais crier victoire trop vite) : aucune attaque majeure n'a touché l'établissement. Seules quelques alertes de type P2 ont été relevées et stoppées suffisamment tôt.

A la Réunion, le déploiement s'est fait par étapes. D'abord les 6 500 postes de travail du CHU, puis les serveurs (en mode "détection"), ensuite l'ensemble des établissements du GHT. Désormais, tout le parc PC est couvert et le parc de serveurs de manière partielle. En plus du service managé d'EDR, les établissements sont passés au format XDR (Extended Detection and Response). Modification sur l'active directory, activité sur le firewall sont ainsi également passées au crible. « Plus on a de traces, d'événements analysés, plus notre détection sera rapide et efficace ». Dans cette logique, le périmètre couvert devrait encore s'étendre. La surveillance des sondes NDR (qui analysent le trafic sur le réseau) apportera prochainement une nouvelle touche à la cybersécurité des établissements réunionnais. « Le marché, tel qu'il est construit, permet d'avancer pas à pas, précise le RSSI. Il est modulable car conçu par briques. Nous allons continuer d'étendre progressivement son champ car nous n'avons pas les ressources nécessaires en interne. Nous avons besoin de nous appuyer sur ces équipes d'experts, disponibles 24h/24 et 7j/7. »

Marion BOIS

Ivan Paturel
Directeur technique et RSSI du CHU Grenoble-Alpes et du GHT Alpes Dauphiné
Crédit photo : DR

Frederic Descamps
Market Manager Public & Healthcare chez Advens
Crédit photo : DR

Stéphane Duchesne
RSSI
GHT de la Réunion
Crédit photo : DR

Jacky Grisey
SOC manager en charge du run service (service de routine) chez Advens
Crédit photo : DR

Thomas Jan
Directeur général adjoint en charge de la stratégie numérique chez UniHA (CAIH)
Crédit photo : DR

En savoir plus